UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/740,400	12/18/2000	Robert Delee Bones	AUS920000798US1	5848

35525 7590 07/13/2005

IBM CORP (YA)
C/O YEE & ASSOCIATES PC
P.O. BOX 802333
DALLAS, TX 75380

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 07/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/740,400
Filing Date: December 18, 2000
Appellant(s): BONES ET AL.

James O. Skarsten
Registration No. 28,346
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 5/24/2005.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

A statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief.

(3) Status of Claims

The statement of the status of the claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Invention

The summary of invention contained in the brief is correct.

(6) Issues

The appellant's statement of the issues in the brief is correct.

(7) Grounds of Rejection to be Reviewed on Appeal

Claims 1-14, 20-33, 39-52 rejected under 35 U.S.C. 102(b) as being anticipated by He (U.S. Patent 5,944,824) hereinafter referred to as He.

Claims 15, 34, and 53 rejected under 35 U.S.C. 103(a) as being unpatentable over He as applied to claims 5, 24, and 43 respectively above, and further in view of Redpath (U.S. Patent 5,854,629) hereinafter referred to as Redpath.

Claims 16, 35, and 54 rejected under 35 U.S.C. 103(a) as being unpatentable over He as applied to claims 1, 20, and 39 respectively above, and further in view of Prafullchandra (U.S. Patent 5,734,718) hereinafter referred to as Prafullchandra.

Claims 17-19, 36-38, 55-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of He and Prafullchandra as applied to 16, 35, and 54 respectively above.

(8) Claims Appealed

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9) Prior Art of Record

5944824	He	8-1999
5854629	Redpath	12-1998
5734718	Prafullchandra	3-1998

(10) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-14, 20-33, 39-52 rejected under 35 U.S.C. 102(b) as being anticipated by He (U.S. Patent 5,944,824) hereinafter referred to as He.

Claim 1 recites changing the SSO password in response to receiving a change instruction. He disclosed a programmed method and system for changing passwords in a Single Sign-On (SSO) environment (See He Col. 13 Paragraphs 3-7). He disclosed that in response to a request to modify a user account (See He Col. 13 Lines 12-13) a new password is generated (See He Col. 13 Lines 20-22) and the old password is set to the new password (See He Col. 13 Lines 43-45).

Claim 1 further recites retrieving and modifying a target password. He disclosed retrieving the target password (See He Col. 13 Lines 22-25). He Further disclosed changing a target NE password to the specified new password (See He Col. 13 Lines 31-35).

Regarding claims 2-4, He disclosed providing the modified password target password to the network element, or client (See He Col. 10 Paragraphs 2-3). It is inherent that the password was first stored in order for it to have been provided in the ticket, as is specified by He (See He Col. 10 Lines 16-21).

Regarding claims 5, 8-9, He disclosed password generation by a random number generator or by manually entering the password (See He Col. 13 Paragraph 4). Because this task was carried out by the network security administrator (See He Col. 13 Paragraph 3), it was inherent that a menu was provided such that the password generation method could be chosen.

Regarding claims 6-7, He disclosed users using one password for multiple applications (See He Col. 1 Paragraph 5).

Regarding claim 10, He disclosed random password generation being performed in a server (See He Col. 11 Lines 40-41).

Regarding claim 11, He disclosed the use of password policy in generating the random passwords (See He Col. 12 Paragraph 2). It is inherent that the password policy was determined in order for it to have been used.

Regarding claim 12-14, He disclosed different types of passwords. He disclosed standard user passwords (See He Col. 11 Paragraph 2), network element passwords (See He Col. 8 Paragraph

8), and Super-User passwords (See He Col. 8 Paragraph 8). It was inherent that each of these groups had some sort of password policy to be checked against (See He Col. 12 Paragraph 2).

Regarding claims 20-33, He disclosed a programmed method and system for changing passwords in a Single Sign-On (SSO) environment (See He Claims 1 and 5). Because He claimed a programmed method to be run in a network, it was inherent that the method comprised a computer program product in computer readable media. Claims 20-33 are therefore rejected for the same reasons as applied to claims 1-14 above.

Regarding claims 39-52, He disclosed a programmed method and system for changing passwords in a Single Sign-On (SSO) environment (See He Claims 1 and 5). Claims 39-52 are therefore rejected for the same reasons as applied to claims 1-14 above.

Claims 15, 34, and 53 rejected under 35 U.S.C. 103(a) as being unpatentable over He as applied to claims 5, 24, and 43 respectively above, and further in view of Redpath (U.S. Patent 5,854,629) hereinafter referred to as Redpath.

Regarding claims 15, 34, and 53:

He disclosed password generation by a random number generator or by manually entering the password (See He Col. 13 Paragraph 4). However, He failed to disclose the use of a Graphical User Interface (GUI) for implementing this selection.

Redpath teaches that GUIs were created in order to simplify interaction with computer programs for end users of computer programs, such that end users do not need to know specific commands in order to effectively use the computer program (See Redpath Col. 1 Paragraph 2).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Redpath in the invention of He such that the user is supplied a GUI menu in order to select a password generation method. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide a simple interface for the user to interact with the password-changing program.

Claims 16, 35, and 54 rejected under 35 U.S.C. 103(a) as being unpatentable over He as applied to claims 1, 20, and 39 respectively above, and further in view of Prafullchandra (U.S. Patent 5,734,718) hereinafter referred to as Prafullchandra.

Regarding claims 16, 35, and 54:

He disclosed retrieving and changing target passwords (See He Col. 13 Paragraphs 3-7), but He failed to disclose a change target password policy. However, He did disclose that having different administrative policies in individual network elements can be problematic (See He Col. 1 Paragraph 5).

Prafullchandra teaches that requiring users to change passwords at predetermined intervals can enhance system security (See Prafullchandra Col. 2 Paragraph 3).

It would have been obvious to the ordinary person skilled in the art at the time of the invention to employ the password aging and changing policy of Prafullchandra to the password changing system and method of He. This would have been obvious because the ordinary person skilled in the art would have been motivated to enhance the security in the network of He.

Claims 17-19, 36-38, 55-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of He and Prafullchandra as applied to 16, 35, and 54 respectively above.

He disclosed different types of passwords. He disclosed standard user passwords (See He Col. 11 Paragraph 2), network element passwords (See He Col. 8 Paragraph 8), and Super-User passwords (See He Col. 8 Paragraph 8).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the policy determination method of Prafullchandra to all the types of passwords of He. This would have been obvious because the ordinary person skilled in the art would have been motivated to enhance the security of all the passwords, regardless of their type.

(11) Response to Argument

The appellant has presented four different issues, the examiner is selecting claim 1 to be representative of Issue #1, claim 15 to be representative of Issue #2, claim 16 to be representative of Issue #3, and claim 17 to be representative of Issue #4.

Issue #1

The examiner notes that the arguments with regards to claim 1 presented in the Appeal Brief are very similar to the arguments presented in the Communication dated 8/16/2004, which were addressed in the "Response to Arguments" section in the Final Action dated 11/24/2004. The examiner further notes that these Responses have not yet been addressed by the Appellants.

It is first important to note the term pairing below which maps the main nouns of the claims to the main nouns of He.

Term Pairing Between the Claimed Subject Matter and He (See Fig. 3).

First Single Sign-on Password	Present Password in Network Element 20
Second Single Sign-on Password	New Password
Target Password	Present Password in the Record stored at the Security Server 15

As can be seen from the above mapping, He disclosed two "Present Passwords". The first "Present Password" is the located in Network Element 20 depicted in Fig. 3. He disclosed that, conventionally, users require multiple user identifiers and passwords to be used on different Network Elements respectively (See He Col. 1 Lines 59-60) and that Single Sign-On capability performs authentication into a Network Element automatically and transparently on behalf of the user (See He Col. 2 Lines 48-50 and 57-59). He further disclosed that for a user with SSO capability, one Present Password for the user was located in the Network Element 20 (See He Col. 7 Lines 64-65). He also disclosed that a second "Present Password" was located in a record stored in a database 13 in a security server 15 (See He Col. 10 Lines 38-44 and Line 66 – Col. 11

Line 2). This distinction between the first "Present Password" in the Network Element 20 and the second "Present Password" in the Record stored at the Security Server 15 is very important to the understanding of the disclosure of He and how it maps to the claim language of the rejected claims.

The appellants argue that He did not disclose "in response to receiving a change instruction identifying a first single sign-on password, changing the first single sign-on password to create a second single sign-on password". As can be seen in Col. 13 of He, He disclosed sending a message identifying the "Present Password" in the Network Element 20 to a "secure terminal server" 24 (See He Col. 13 Lines 26-30). Although this message was not specifically called a "change instruction", the message resulted in the changing of passwords at the Network Element, as can be seen in Col. 13 Lines 31-35. Col. 13 Lines 31-35 further show that upon receiving this message (or in response to the message), the "secure terminal server" changed the Present Password (First SSO Password) in the Network Element 20 to the New Password (Second SSO Password) using the data provided in the message of Col. 13 Lines 27-28.

The appellants argue that He did not disclose "modifying the target password in a user selected manner to match the second single sign-on password to create a modified target password". He disclosed in Col. 13 Lines 38-39 that the Present Password in the retrieved record (Target Password) was modified to match the New Password (Second SSO Password). Although, He did not specifically disclose a "modified target password", after the Present Password in the record was changed to match the New Password, it constituted a modified target

password because it was different than it was when the process started. Furthermore, in Col. 13 Lines 20-22, He disclosed that new passwords could be generated manually, which constituted a user-defined manner.

The appellants argue that He does not relate to changing an SSO Password. As can be seen from the Title of the Invention of He, "System and Method for Single Sign-On to a Plurality of Network Elements", He did disclose a system related to SSO. He further disclosed changing the Present Password of a Super User, which can be seen in Col. 13 Lines 27-28 and 31-35. Furthermore, He disclosed in Col. 8 Lines 47-52, that the Super User could have SSO capability, and, in Col. 2 Lines 28-31 and 47-50, that SSO capability allowed a user to authenticate once to a network authentication service, at which point a Security Server would authenticate the user into the Network Elements. As such, the system of He did in fact relate to changing SSO Passwords, and more specifically to changing Super User SSO Passwords.

The appellants argue that "He clearly describes that the super user identifier is not a single sign-on password'. The Section cited by the appellants to show this is Col. 11 Lines 3-11, wherein the examiner can find no teaching that He describes that the super user identifier is not a single sign-on password, but the examiner agrees that this may be the case because in general an identifier is not meant to be a password, but is usually associated with a password. However, He clearly disclosed that a Super User had the SSO capability as recited in Col. 8 Lines 47-54, and further that the super user had a password, which was changed (See He Col. 13 Lines 31-35). Further, He disclosed that the secure terminal server logged into the Network Element for the

super user using the super user identifier and passwords provided in the message of Col. 13 Lines 27-28 (See He Col. 13 Lines 31-35), and that the SSO login to a Network Element was performed automatically by a security server (See He Col. 2 Lines 25-32). In comparing these two login descriptions, it is clear that the super user of Col. 13 Paragraphs 3-7 was an SSO super user and the passwords were SSO passwords. Further still, He Col. 8 Lines 58-60 disclose that the SSO super user is used for automatic Network Element user password initialization and recovery, which is what the system/method of Col. 13 Paragraphs 3-7 is accomplishing (See Col. 13 Lines 10-11).

The appellants argue again that He did not disclose changing a first SSO password to a second SSO password. As discussed above, the passwords of Col. 13 Paragraphs 3-7 were SSO passwords and therefore, as discussed above, He did disclose changing a first SSO password to a second SSO password (Present Password in the Network Element 20 to the New Password).

The appellants argue again that He did not disclose modifying the target password in a user selected manner to match the second single sign-on password to create a modified password. This argument has been addressed above and will not be addressed further.

The appellants again argue that He did not disclose "in response to receiving a change instruction identifying a first single sign-on password, changing the first single sign-on password to create a second single sign-on password". This argument has been addressed above and will not be addressed further.

These arguments also apply to dependant claims 2-14, claims 20-33 and claims 39-52.

Issue #2

The appellants argue that because claim 15 depends from claim 1, the arguments for claim 1 above also apply to claim 15. As such, the response to the arguments in view of claim 1 also apply to claim 15, as well as claims 34, and 53.

Issue #3

The appellants argue that because claim 16 depends from claim 1, the arguments for claim 1 above also apply to claim 16. As such, the response to the arguments in view of claim 1 also apply to claim 16, as well as claims 35, and 54.

The appellants further argue that Prafullchandra does not discuss that "in response to a determination that a target password has been retrieved", "determining a change target password policy" and "applying the change target password policy to modify the target password to match the second single sign-on password to create the modified target password". In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Claims 16, 35, and 54 were rejected in view of the combination of He and Prafullchandra and as such cannot be expected to each individually teach all of the

limitations of the claim. However, these limitations were met by the combination as a whole. He disclosed retrieving a target password (See He Col. 13 Lines 22-25 "Present Password" of the record) and modifying the target password in a user selected manner to match the second single sign-on password to create a modified target password (See He Col. 13 Lines 38-39 wherein in the Present Password in the retrieved record was modified to match the New Password. Although, He did not specifically disclose a "modified target password", after the Present Password in the record was changed to match the New Password, it constituted a modified target password because it was different than it was when the process started. Also, in Col. 13 Lines 20-22, He disclosed that new passwords could be generated manually, which constituted a user-defined manner), while Prafullchandra taught a password aging method for changing passwords in which upon receipt of a username and password (See Prafullchandra Col. 6 Lines 8-9 and 13-16), determining whether the aging password change policy will be used or not in the password change (determining a change target password policy) (See Prafullchandra Col. 6 Lines 46-57), and changing the password based on the policy decision (applying the change target password policy) (See Prafullchandra Col. 6 Line 59 – Col. 7 Line 2 and Figs. 5b and 5c Especially Steps 80-90). In this combination, the password change policy was determined based upon whether aging will be used or not and after determining the policy it was applied and the target password (Present Password in the Record) was changed to match the second password (New Password) which created a modified target password. Further, it was obvious that the determination, that the record or He was received, was made, prior to attempting to alter the target password in the record.

Issue #4

The appellants argue that because claim 17-19 depend from claim 16, the arguments for claim 16 above also apply to claims 17-19. As such, the response to the arguments in view of claim 1 and 16 also apply to claims 17-19, as well as claims 36-38, and 55-57.

In summary, the examiner addressed the appellants' arguments:

As per Issue #1, the examiner has shown that He disclosed a first SSO password, a second SSO password and a target password and has addressed the arguments pertaining to changing a first SSO password to a second SSO in response to receiving a change instruction and modifying a target password to match the second password. The examiner further addressed the arguments pertaining to whether the super user passwords were SSO passwords, and the arguments pertaining to the super user identifier not being an SSO password. The examiner has further provided support showing that He has been properly applied.

As per Issue #2, the examiner has followed the appellants lead and shown that the arguments pertaining to Issue #1 further apply to dependant claims 15, 34, 53.

As per Issue #3, the examiner has addressed the appellants' arguments pertaining to Prafullchandra not teaching all the limitations of claims 16, 35, and 54 and has shown that the limitations were obvious in view of the combination of He and Prafullchandra.

As per Issue #4, the examiner has followed the appellants lead and shown that the arguments pertaining to Issue #3 further apply to dependant claims 17-19, 36-38, and 55-57.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

MTH

June 30, 2005

Conferees:

Christopher Revak AU2131 7/11/05
Ayaz Sheikh

IBM CORP (YA)
C/O YEE & ASSOCIATES PC
P.O. BOX 802333
DALLAS, TX 75380

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100